UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/666,843	09/19/2003	William E. Sobel	SYMAP033	5791

21912 7590 02/18/2009
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
ARMOUCHE, HADI S	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
02/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/666,843	**Applicant(s)** SOBEL, WILLIAM E.
	Examiner HADI ARMOUCHE	**Art Unit** 2432

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 November 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-11,13,14 and 16-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-11,13,14 and 16-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 September 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This communication is in response to applicant's amendment filed on 11/26/2008. Claim 12 has been cancelled, claims 1, 14 and 16 have been amended. Claims 1-7, 9-11, 13-14 and 16-22 remain pending.

2. Applicant's amendment to claims 1, 14 and 16 obviate previously raised rejection under 35 USC 112, 2nd paragraph. Rejection under 35 USC 112, 2nd paragraph is hereby withdrawn.

Specification

3. The disclosure is objected to because of the following informalities:

- The specification page 6 line 3 discloses:"...remote addresses 108-118.." which suggests that there are remote addresses 109, 111, 113, 115 and 117 which is not the case. Please say: "108, 110, 112, 114, 116 and 118". Similarly on page 6 line 3, 4, 5-6, 7-8, 8, page 8 lines 18, 19, 21, page 9 lines 2, 8, 11, 14, 15, page 10 lines 9, 17, page 11 line 3 and page 13 lines 10-11 .
- The specification page 8 line 16 and page 13 line 18 refer to Fig1. It should say Fig 1A since Fig1 doesn't exist.
- The specification page 15 line 5 refers to RAU by 203. It should be labeled 206 to be consistent with earlier references and figure 2. Appropriate correction is required.

Response to Arguments

4. Applicant's arguments filed 11/26/2008 have been fully considered but they are not persuasive.

5. It has been argued (page 6 of the remarks) that the amendment recitation "properly authenticated pattern of connection requests, probes, and scans" is not taught by either Kalajan or Teraoka. Instead, Kalajan discloses using password systems to validate communication packets and Teraoka teaches the usage of "source-host authenticator" within a packet header that contains a "predetermined secret key" used for authentication purpose.

6. Applicant's interpretation of the references is noted. However, the specification of the current application page 7 lines 11-15 states:

> Authentication techniques can include the use of other patterns and techniques such as hash values, behavioral combinations (e.g., data packets sent to a port in a pre-defined sequence), pre-defined passwords, shared secrets, and authorized address lists. Other techniques may include passwords that can be converted into a series of operations or other passwords.

Kalajan disclose password systems as a means for validation of communication packets (see column 4, lines 1-15). However Teraoka specifically identifies a source-host authenticator within in the packet header which is used for authentication purposes. Teraoka's source-host authenticator contains a predetermined secret key (Ks) which is well known in the art to be equivalent to a password (see column 7, line 47). Furthermore, the source-host authenticator is calculated by computing a checksum (which is also well known in the art to ensure data integrity and error detection) and the secret key of the data packet (see column 7, lines 59-64). Therefore, it would have been obvious to authenticate a source-host (i.e. port) using pre-defined passwords.

7. It has been argued (page 6 of the remarks) that the amendment recitation "allowing the remote address to establish, through a connection request received during the configurable period of time, a connection with the host via a port with which the request is associated and closing the port after expiration of the configurable period of time" is not taught by either Kalajan or Teraoka.

8. Applicant's interpretation of the references is noted. However, Kalajan teaches this feature in column 1 line 65-column 2 line 8, column 2 lines 61-64 and column 4 line 66-column 5 line 4 as describe below.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 1-7, 9 – 11, 13-14, and 16 – 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kalajan in US Patent No. 6202156 (hereinafter US '156) further in view of Teraoka in US Patent No. 6009528 (hereinafter US '528).

10. For claim 1, and similar independent claims 14 and 16, US '156 discloses:

A method for network security comprising:

receiving a request from a remote address at a host;

observing a behavioral pattern of packets associated with the request;

authenticating the remote address based on the behavioral pattern of the packets associated with the request; and

enabling access to the host by the remote address for a configurable time period if the remote address is authenticated; (see Abstract; Figure 1; column 1, lines 35 – 63, 65 – column 2, lines 1 – 10, 29 – 34, 37 – 43, 50 – 58: process of validating access request…, 60 – 65: time period…; column 6, lines 47 – 51: packet observation…)

and wherein enabling access comprising allowing the remote address to establish, through a connection request received during the configurable period of time, a connection with the host via a port with which the request is associated and closing the port after expiration of the configurable period of time. (see column 1 line 65-column 2 line 8, column 2 lines 61-64 and column 4 line 66-column 5 lines 1-4).

but does not expressly disclose wherein the authentication is based at least in part a determination that the observed behavioral pattern of the packets matches a properly authenticated pattern of connection requests, probes, or scans;

(Kalajan et al discloses that password systems as a means for validation of communication packets (see column 4, lines 1-15).

Teraoka however in US '528 teaches wherein the authentication is based at least in part a determination that the observed behavioral pattern of the packets matches a properly authenticated pattern of connection requests, probes, or scans. (see Abstract; column 7, lines 43 – 46: authentication information is in the packet header; column 7, lines 53 – 58: packet header contents; column 9, lines 16 – 23: packet header authentication and see column 7, lines 53-58: source-host authenticator includes predetermined secret key (see column 7, line 47, 60-65)).

Kalajan and Teraoka are analogous art because they are from the same problem solving areas (enhancing the security of communication on a network). At the time of the invention, it would have been obvious to a skilled artisan to modify the method of packet authentication of Kalajan such "that it would be based at least in part a determination that the observed behavioral pattern of the packets matches a properly authenticated pattern of connection requests, probes, and scans" such as packet header authentication as in Teraoka. The motivation for doing so would have been to enhance network security.

11. For claim 2, and similar claim 17, US '156 teaches:

A method for preventing network discovery of a system services configuration as recited in claim 1 further including preventing a response from being sent to the remote address. (see column 1, lines 36 – 37; column 3, lines 17 – 20)

12. For claim 3, and similar claim 18, US '156 discloses:

A method for preventing network discovery of a system services configuration as recited in claim 1 wherein receiving a request from a remote address at the host further includes receiving a probe. (see column 2, lines 42 – 43; column 4, lines 41 – 43, 58 – 61)

13. For claim 4, and similar claim 19 US '156 discloses:

A method for preventing network discovery of a system services configuration as recited in claim 1 wherein observing a pattern associated with the request further includes recording data received at the host. (see column 4, lines 33: firewall; column 6, lines 47 – 56)

14. For claim 5, and similar claim 20, US '156 teaches:

A method for preventing network discovery of a system services configuration as recited in claim 1 wherein observing a pattern associated with the request further includes matching the pattern to a list. (see column 4, lines 1 – 11)

15. For claim 6, US '156 teaches:

A method for preventing network discovery of a system services configuration as recited in claim 1 wherein observing a pattern associated with the request further includes recording a sequence. (see column 4, lines 1 – 11, 35 – 39 and 54 -61)

16. For claim 7, and similar claim 21 US '156 teaches:

A method for preventing network discovery of a system services configuration as recited in claim 1 wherein authenticating the remote address based on the pattern associated with the request further includes comparing the pattern to a list. (see column 4, lines 1 – 11 and 54 – 61)

17. For claim 9, and similar claim 22 US '156 discloses:

A method for preventing network discovery of a system services configuration as recited in claim 1 wherein authenticating the remote address based on the pattern associated with the request further includes preventing a response being sent to the remote address if the remote address fails to authenticate. (see column 4, lines 62 – 65: blocked by firewall; column 5, lines 53 – 56)

18. For claim 10, US '156 teaches:

A method for preventing network discovery of a system services configuration as recited in claim 1 wherein authenticating the remote address based on the pattern associated with the request further includes denying access to the host if the remote address fails to authenticate. (see column 5, lines 53 – 56 and 65 - column 6, lines 1-7)

19. For claim 11, US '156 teaches:

A method for preventing network discovery of a system services configuration as recited in claim 1 wherein authenticating the remote address based on the pattern associated with the request further includes sending a message to the remote address if the request fails to authenticate. (see column 5, lines 53 – 56 and 65 - column 6, lines 1-7)

20. For claim 13, US '156 discloses:

A method for preventing network discovery of a system services configuration as recited in claim 1 wherein enabling access to the host by the remote address further includes implementing a handshake between the remote address and the host. (see column 4, lines 54 –58)

Conclusion

21. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is (571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432
02/12/2009

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432